

Cisco ISE 2.7 Admin Guide: Device Administration

Device Administration

TACACS+ Device Administration

Cisco ISE supports device administration using the Terminal Access Controller Access-Control System (TACACS+) security protocol to control and audit the configuration of network devices. The network devices are configured to query ISE for authentication and authorization of device administrator actions, and send accounting messages for ISE to log the actions. It facilitates granular control of who can access which network device and change the associated network settings. An ISE administrator can create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service. The ISE Monitoring node provides enhanced reports related to device administration. The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators.

ISE requires a Device Administration license to use TACACS+.

There are two types of administrators for device administration:

- Device Administrator
- ISE Administrator

The device administrator is the user who logs into the network devices such as switches, wireless access points, routers, and gateways, (normally through SSH), in order to perform the configuration and maintenance of the administered devices. The ISE administrator logs into ISE to configure and coordinate the devices that a device administrator logs in to.

The ISE administrator is the intended reader of this document, who logs into ISE to configure the settings that control the operations of the device administrator. The ISE administrator uses the device administration features (Work centers > Device Administration) to control and audit the configuration of the network devices. A device can be configured to query the ISE server using the Terminal Access Controller Access-Control System (TACACS) security protocol. The ISE Monitoring node provides enhanced reports related to device administration. An ISE administrator can perform the following tasks:

- Configure network devices with the TACACS+ details (shared secret).
- Add device administrators as internal users and set their enable passwords as needed.
- Create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service.
- Configure the TACACS server in ISE to allow device administrators to access devices based on the policy sets.

The device administrator performs the task of setting up a device to communicate with the ISE server. When a device administrator logs on to a device, the device queries the ISE server, which in turn queries an internal or external identity store, to validate the details of the device administrator. When the validation is done by

the ISE server, the device informs the ISE server of the final outcome of each session or command authorization operation for accounting and auditing purposes.

An ISE administrator can manage device administration using TACACS and Cisco ISE 2.0 and later releases. The configuration related to device administration can also be migrated from a Cisco Secure Access Control System (ACS) server, versions 5.5, 5.6, 5.7 and 5.8. Prior versions need to be upgraded to 5.5 or 5.6 before migration.



Note You should check the **Enable Device Admin Service** check box in the **Administration > System > Deployment > General Settings** page to enable TACACS+ operations. Ensure that this option is enabled in each PSN in a deployment.

Due to a known limitation of TACACS+ protocol to create a secure connection between switch or router and ISE, ensure that IPsec protocol is deployed between the two parties.



Note Cisco ISE requires a Device Administration license to use the TACACS+ service on top of an existing Base or Mobility license. The Device Administration license is a perpetual license. If you are upgrading from an earlier release to Cisco ISE Release 2.0 and later, and would like to enable the TACACS+ service, you must order the Device Administration license as a separate add-on license. The number of Device Administration licenses must be equal to the number of device administration nodes in a deployment.

[ISE Community Resource](#)

For information about device administration attributes, see [ISE Device Administration Attributes](#).

For information about TACACS+ configuration for Wireless LAN controllers, IOS network devices, Cisco NX-OS network devices, and network devices, see [ISE Device Administration \(TACACS+\)](#).

Device Administration Work Center

The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators. However, pages that are not specific to device administration such as Users, User Identity Groups, Network Devices, Default Network Devices, Network Device Groups, Authentication and Authorization Conditions, can still be accessed from their original menu options, such as Administration. The Work Centers option is available only if the correct TACACS+ license(s) are obtained and installed.

The Device Administration Menu contains the following menu options: Overview, Identities, User Identity Groups, Ext ID Stores, Network Resources, Network Device Groups, Policy Elements, Device Admin Policy Sets, Reports, and Settings.

Device Administration Deployment Settings

The Device Administration Deployment page (**Work Centers > Device Administration > Overview > Deployment**) allows ISE administrators to centrally view the device administration system without referring to each node in the deployment section.

The Device Administration Deployment page lists the PSNs in your deployment. This simplifies the task of enabling the device admin service individually in each PSN in your deployment. You can collectively enable the device admin service for many PSNs by selecting an option below:

Option	Description
None	By default, the device administration service is disabled for all nodes.
All Policy Service Nodes	Enables the device administration service in all PSNs. With this option, new PSNs are automatically enabled for device admin when they are added.
Specific Nodes	Displays the ISE Nodes section that lists all the PSNs in your deployment. You can select the required nodes that necessitate the device admin service to be enabled.



Note If the deployment is not licensed for TACACS+, the above options are disabled.

The TACACS Ports field allows you to enter a maximum of four TCP ports, which are comma-separated and port values range from 1 to 65535. Cisco ISE nodes and their interfaces listen for TACACS+ requests on the specified ports and you must ensure that the specified ports are not used by other services. The default TACACS+ port value is 49.

When you click **Save**, the changes are synchronized with the nodes specified in the **Administration > System > Deployment Listing** page.

Device Admin Policy Sets

The Device Admin Policy Sets page (Work Centers > Device Administration > Device Admin Policy Sets) contains the list of policy sets that an ISE administrator manages to control the authentication and authorization of TACACS+ Device administrators. Each policy can be in one of two modes: Regular and Proxy Sequence.

A Regular policy set comprises an authentication rule table and an authorization rule table. The authentication rule table contains a set of rules to select actions required to authenticate a network device.

The authorization rule table contains a set of rules to select the specific authorization results required to implement the authorization business model. Each authorization rule consists of one or more conditions that must be matched for the rule to be engaged, and a set of command sets, and/or a shell profile, which are selected to control the authorization process. Each rule table has an exception policy that can be used to override the rules for specific circumstances, often the exception table is used for temporary situations.

A Proxy Sequence policy set contains a single selected proxy sequence. If the policy set is in this mode then the remote proxy server(s) are used to process the requests (although local accounting may be configured by the Proxy Sequence).


Create Device Administration Policy Sets

To create a device administration policy set:

Before you begin

- Ensure that the Device Administration in the **Work Centers > Device Administration > Overview > Deployment** page is enabled for TACACS+ operations.
- Ensure that any User Identity Groups, (for example, System_Admin, Helpdesk) required for the policy are created. (**Work Centers > Device Administration > User Identity Groups** page). Ensure that the member users (for example, ABC, XYZ) are allocated to their corresponding groups. (**Work Centers > Device Administration > Identities > Users** page).
- Ensure to configure TACACS settings on devices that need to be administered. (**Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS Authentication Settings** check box is enabled and the shared secret for TACACS and devices are identical to facilitate the devices to query ISE.)
- Ensure that the Network Device Group, based on the Device Type and Location, is created. (**Work Centers > Device Administration > Network Device Groups** page)

Procedure

-
- Step 1** Choose **Work Centers > Device Administration > Device Admin Policy Sets**.
- Step 2** From the **Actions** column on any row, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary. A new row appears in the Policy Sets table.
- Step 3** Enter the name and description for the policy set.
- Step 4** If required, from the Allowed Protocols/Server Sequence column, click the (+) symbol and select one of the following:
- a) Create a New Allowed Protocol
 - b) Create a TACACS Server Sequence
- Step 5** From the **Conditions** column, click the (+) symbol.
- Step 6** Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Device-Location Equals Europe).
You can drag and drop a Library condition to the **Click To Add An Attribute** text box.
- Step 7** Click **Use**.
- Step 8** From the View column, click  to access all of the policy set details and to create the authentication and authorization policies as well as policy exceptions.
- Step 9** Create the required Authentication policy, (for example, Rule Name: ATN_Internal_Users, Conditions: DEVICE:Location EQUALS Location #All Locations#Europe—The policy matches only devices that are in location Europe).
- Step 10** Click **Save**.
- Step 11** Create the required Authorization Policy.
Example 1: Rule Name: Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8—The policy matches system administrators with user name ABC and allows the specified commands to be executed and assigns a privilege level of 8.

Example 2: Rule Name: HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1—The policy matches system administrators with user name XYZ and allows the specified commands to be executed and assigns a privilege level of 1.

In the above examples:

- The command sets, cmd_Sys_Admin and cmd_HDesk, are created in the **Work Centers > Device Administration > Policy Elements > Results>TACACS Command Sets > Add** page.
- The TACACS profiles, Profile_Priv_1 and Profile_priv_8, are created in the **Work Centers > Device Administration > Policy Elements > Results >TACACS Profiles > Add** page.

Note You can add IPv4 or IPv6 single address for the Device IP address attribute in the conditions used in authentication and authorization policies.

Step 12 Click **Save**.

TACACS+ Authentication Settings and Shared Secret

The following table describes the fields on the Network Devices page, which you can use to configure TACACS+ authentication settings for a network device. The navigation path is:

- (For Network Devices) **Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS Authentication Settings**.
- (For Default Devices) **Work Centers > Device Administration > Network Resources > Default Devices > TACACS Authentication Settings**. See the "Default Network Device Definition in Cisco ISE" section in for more information.

Field	Usage Guidelines
Shared Secret	A string of text assigned to a network device when TACACS+ protocol is enabled. A user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret. This is not a mandatory field.
Retired Shared Secret is Active	Displayed when the retirement period is active.
Retire	Retires an existing shared secret instead of ending it. When you click Retire, a message box is displayed. You can either click Yes or No .

Field	Usage Guidelines
Remaining Retired Period	(Available only if you select Yes in the above message box) Displays the default value specified in the following navigation path: Work Centers > Device Administration > Settings > Connection Settings > Default Shared Secret Retirement Period . You can change the default values. This allows a new shared secret to be entered and the old shared secret will remain active for the specified number of days.
End	(Available only if you select Yes in the above message box) Ends the retirement period and terminates the old shared secret.
Enable Single Connect Mode	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one of the following: <ul style="list-style-type: none"> • Legacy Cisco Devices • Or, TACACS+ Draft Compliance Single Connect Support. If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request.

In summary, you can

- Retire the old shared secret by specifying the retirement period as number of days (Range is 1 to 99) and at the same time set a new shared secret.
- Use the old and new shared secrets during the retirement period.
- Extend the retirement period before it expires.
- Use the old shared secret only until the end of the retirement period.
- Terminate the retirement period before it expires (click End and then Submit).



Note The TACACS+ Authentication Settings option can also be accessed from the **Administration > Network Resources > Network Devices > Add** page.

Device Administration - Authorization Policy Results

ISE administrators can use the TACACS+ command sets and TACACS+ profiles (policy results) to exercise control over the privileges and commands that are granted to a device administrator. The policy works in conjunction with the network devices and thereby prevents accidental or malicious configuration changes that

may be done. In the event such changes occur, you can use the device administration audit reports to track the device administrator who has executed a particular command.

Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration

There are many allowed authentication protocol services that Cisco ISE offers for creating the policy results. However, authentication protocol services such as PAP/ASCII, CHAP, and MS-CHAPv1, which are applicable to the TACACS+ protocol, are disabled on FIPS-enabled Cisco ISE appliances for RADIUS. As a result, these protocols cannot be enabled in the **Policy > Policy Elements > Results > Allowed Protocols** page to administer devices, when using a FIPS-enabled (**Administration > System Settings > FIPS Mode**) Cisco ISE appliance.

Consequently, to configure PAP/ASCII, CHAP, and MS-CHAPv1 protocols in your device administration policy results, for both FIPS and non-FIPS modes, you must navigate to the **Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols** page. Only the Default Device Admin allowed protocols setting may be used when FIPS mode is enabled. This option is not allowed in RADIUS.

TACACS+ Command Sets

Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.

Wildcards and Regex in Command Sets

A command line comprises the command and zero or more arguments. When Cisco ISE receives a command line (request), it handles the command and its arguments in different ways:

- It matches the command in the request with the commands specified in the command set list using the wildcard matching paradigm.
Example: Sh?? or S*
- It matches the arguments in the request with the arguments specified in the command set list using regular expressions (regex) matching paradigm.
Example: Show interface[1-4] port[1-9]:tty*

Command Line and Command Set List Match

To match a requested command line to a command set list containing wildcards and regex:

1. Iterate over a command set list to detect matching commands.

Wildcard matching permits:

- Case insensitivity
- Any character in the command in the command set may be "?", which matches any individual character that must exist in the requested command
- Any character in the command in the command set may be "*", which matches zero or more characters in the requested command

Examples:

Request	Command Set	Matches	Comments
show	show	Y	—
show	SHOW	Y	Case insensitive
show	Sh??	Y	Matches any character
show	Sho??	N	Second "?" intersects with the character that does not exist
show	S*	Y	"*" matches any character
show	S*w	Y	"*" matches characters "ho"
show	S*p	N	Character "p" does not correspond

- For each matching command, Cisco ISE validates the arguments.

The command set list will include a space-delimited set of arguments for each command.

Example: Show interface[1-4] port[1-9]:tty.*

This command has two arguments.

- Argument 1: interface[1-4]
- Argument 2: port[1-9]:tty.*

The command arguments in the request are taken in the position-significant order they appear in the packet. If all the arguments in the command definition match the arguments in the request, then this command/argument is said to be matched. Note that any extraneous arguments in the request are ignored.



Note Use the standard Unix regular expressions in arguments.

Process Rules with Multiple Command Sets

- If a command set contains a match for the command and its arguments, and the match has Deny Always, ISE designates the command set as Commandset-DenyAlways.
- If there is no Deny Always for a command match in a command set, ISE checks all the commands in the command set sequentially for the first match.
 - If the first match has Permit, ISE designates the command set as Commandset-Permit.
 - If the first match has Deny, ISE designates the command set as Commandset-Deny.
- After ISE has analyzed all the command sets, it authorizes the command:
 - If ISE designated any command set as Commandset-DenyAlways, ISE denies the command.

- b. If there is no Commandset-DenyAlways, ISE permits the command if any command set is Commandset-Permit; otherwise, ISE denies the command. The only exception is when the **Unmatched** check box is checked.

Create TACACS+ Command Sets

To create a policy set using the TACACS+ command sets policy results:

Procedure

-
- Step 1** Choose **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**.
- You can also configure TACACS command sets in the **Work Centers > Device Administration > Device Admin Policy Sets** page.
- Step 2** Click **Add**.
- Step 3** Enter a name and description.
- Step 4** Click **Add** to specify the Grant permission, Command, and Argument.
- Step 5** In the **Grant** drop-down, you can choose one of the following:
- **Permit**: To allow the specified command, (for example, permit show, permit con* Argument terminal).
 - **Deny**: To deny the specified command, (for example, deny mtrace).
 - **Deny Always**: To override a command that has been permitted in any other command set, (for example, clear auditlogs)
- Note** Click the action icon to increase or decrease the column width of the Grant, Command, and Argument fields.
- Step 6** Check the **Permit any command that is not listed below** check box to allow commands and arguments that are not specified as Permit, Deny or Deny Always in the Grant column.
-

TACACS+ Profile

TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

- Common tasks
- Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using

the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.

The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

- Shell
- WLC
- Nexus
- Generic

The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using an equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

Create TACACS+ Profiles

To create a TACACS+ profile:

Procedure

-
- Step 1** Choose **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.
You can also configure TACACS command sets in the **Work Centers > Device Administration > Device Admin Policy Sets** page.
- Step 2** Click **Add**.
- Step 3** In the **TACACS Profile** section, enter a name and description.
- Step 4** In the **Task Attribute View** tab, check the required **Common Tasks**. Refer to the [Common Tasks Settings, on page 10](#) page.
- Step 5** In the **Task Attribute View** tab, in the **Custom Attributes** section, click **Add** to enter the required attributes.
-

Common Tasks Settings

Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add** to view the common tasks settings page. The Common Task Types are Shell, WLC, Nexus, and Generic.

Shell

The following options are available for the ISE administrator to set the device administrator's privileges.

Option	Description
Default Privilege	Enable the default (initial) privilege level for a device administrator for the shell authorization. Select any one of the following options: <ul style="list-style-type: none"> • Select values between 0 through 15. • Select the required Identity Store Attribute.
Maximum Privilege	Enable the maximum privilege level for Enable authentication. You can select values between 0 through 15.
Access Control List	Select an ASCII String (1-251*) or the required Identity Store Attribute.
Auto Command	Select an ASCII String (1-248*) or the required Identity Store Attribute.
No Escape	Select any one of the following options for escape characters: <ul style="list-style-type: none"> • True—Specifies that escape prevention is enabled. • False—Specifies that escape prevention is not enabled. • Select the required Identity Store Attribute.
Timeout	Select values between 0 through 9999 or the required Identity Store Attribute.
Idle Time	Select values between 0 through 9999 or the required Identity Store Attribute.

WLC

The following options are available for the ISE administrator to control a device administrator's access to the WLC application tabs. The WLC application contains the following tabs: WLAN, Controller, Wireless, Security, Management, and Commands.

Option	Description
All	Device administrators have full access to all the WLC application tabs.
Monitor	Device administrators have only read-only access to the WLC application tabs.
Lobby	Device administrators have only limited configuration privileges.

Option	Description
Selected	Device administrators have access to the tabs as checked by the ISE administrator from the following check boxes: WLAN, Controller, Wireless, Security, Management, and Commands.

Nexus

The following options are available for the ISE administrator to control a device administrator's access to the Cisco Nexus switches.

Option	Description
Set Attribute As	An ISE administrator can specify the Nexus attributes generated by the common tasks as Optional or Mandatory.
Network Role	When a Nexus is configured to authenticate using ISE, the device administrator, by default, has read-only access. Device administrators can be assigned to one of these roles. Each role defines the operations that is allowed: <ul style="list-style-type: none"> • None—No privileges. • Operator (Read Only)— Complete read access to the entire NX-OS device. • Administrator (Read/Write)—Complete read-and-write access to the entire NX-OS device.
Virtual Device Context (VDC)	None— No privileges. Operator (Read Only)— Read access limited to a VDC Administrator (Read/Write)— Read-and-write access limited to a VDC.

Generic

The ISE administrator uses the option to specify custom attributes that are not available in the common tasks.

Access the Command-Line Interface to Change the Enable Password

To change Enable password, perform the following steps:

Before you begin

Some commands are assigned to privileged mode. Therefore, they can only be executed when the device administrator has authenticated into this mode.

The device sends a special enable authentication type when the device administrator attempts to enter the privileged mode. Cisco ISE supports a separate enable password to validate this special enable authentication type. The separate enable password is used when the device administrator is authenticated with internal identity stores. For authentication with external identity stores, the same password is used as for regular login.

Procedure

Step 1 Log in to the switch.

Step 2 Press Enter to display the following prompt:

```
Switch>
```

Step 3 Execute the following commands to configure the Enable password.

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

Note If password lifetime is configured for the Login password and Enable password, the user account will be disabled if the passwords are not changed within the specified time period. If Cisco ISE is configured as TACACS+ server and the **Enable Bypass** option is configured on the network device, you cannot change the Enable password from the CLI (via telnet). Choose **Administration > Identity Management > Identities > Users** to change the Enable password for internal users.

Configure Global TACACS+ Settings

To configure global TACACS+ settings:

Procedure

Step 1 Choose **Work Centers > Device Administration > Settings**.

In the **Connection Settings** tab, you can change the default values for the required fields.

- In the **Authorization cache timeout** field, you can set the Time-To-Live (TTL) value for which certain attributes of an internal user are cached upon the first authorization request. The cached attributes include username, and user-specific attributes, such as UserGroup. These attributes are created under **System Administration > Configuration > Dictionaries > Identity > Internal Users**. The default value is 0, which means the authorization cache is disabled.
- **Single Connect Support**: If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request.

Step 2 In the **Password Change Control** tab, define the required fields to control whether password update is permitted through TACACS+.

The prompts in the **Enable Telnet Change Password** section are enabled only when this option is selected. Or else, the prompts in the **Disable Telnet Change Password** are enabled. The password prompts are fully customizable and can be modified as needed.

In the **Password Policy Violation Message** field, you can display an appropriate error message for the password set by the internal users if the new password does not match the specified criteria.

Step 3 In the **Session Key Assignment** tab, select the required fields to link TACACS+ requests into a session.

The session key is used by the Monitoring node to link AAA requests from clients. The default settings are for NAS-Address, Port, Remote-Address, and User fields to be enabled.

Step 4 Click **Save**.

Related Topics

[TACACS+ Authentication Settings and Shared Secret](#), on page 5

[User Attribute Cache in RADIUS Token Servers](#)

Data Migration from Cisco Secure ACS to Cisco ISE

You can use the migration tool to import data from ACS 5.5 and later, and set default TACACS+ secret for all network devices. Navigate to **Work Centers > Device Administration > Overview** and in the **Prepare** section, click **Download Software Webpage** to download the migration tool. Save the tool to your PC, and from the migTool folder, run the migration.bat file to start the migration process. For complete information related to the migration, refer to the [Migration Guide](#) for your version of ISE.

Monitor Device Administration Activity

Cisco ISE provides various reports and logs that allow you to view information related to accounting, authentication, authorization, and command accounting of devices configured with TACACS+. You can run these reports either on demand or on a scheduled basis.

Procedure

Step 1 Choose **Work Centers > Device Administration > Reports > ISE Reports**.

You can also view the reports in the **Operations > Reports > ISE Reports** page.

Step 2 In the **Report Selector**, expand **Device Administration** to view **Authentication Summary**, **TACACS Accounting**, **TACACS Authentication**, **TACACS Authorization**, **TACACS Command Accounting**, **Top N Authentication by Failure Reason**, **Top N Authentication by Network Device**, **Top N Authentication by User** reports.

Step 3 Select the report and choose the data with which you want to search using the **Filters** drop-down list.

Step 4 Select the **Time Range** during which you want to view the data.

Step 5 Click **Run**.

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs page, which displays the TACACS+ AAA details. The navigation path for this page is: **Operations > TACACS Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 1: TACACS Live Logs

Fields	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is required and cannot be deselected.
Status	Shows if the authentication was successful or a failure. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information on the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows user names who have passed or failed authentication, authorization, or both. This column is required and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE Node through which the access request is processed.
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.

Fields	Usage Guidelines
Network Device Groups	Shows the name of the corresponding network device group to which a network device belongs.
Device Type	Shows the device type policy used to process access requests from different network devices.
Location	Shows the location based policy used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present or shows an empty value if the MatchedCommandSet attribute value is empty or attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the TACACS Live Logs page:

- Export the data in csv or pdf format.
- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.



Note All the user customizations will be stored as user preferences.

Related Topics

[TACACS+ Device Administration](#)

[Configure Global TACACS+ Settings](#), on page 13

